REMARKS

The Office Action dated December 3, 2004 has been received and carefully noted. The above amendments and the following remarks are submitted as a full and complete response thereto.

The specification is amended and claims 4, 5, 7, 9, 11, 14, 15, 19, 25, 28, and 31 are amended to particulary point out and distinctly claim the subject matter of the invention. No new matter is added. Claims 1-32 are respectfully submitted for consideration.

The Office Action objected to the drawings because of informalities. It is respectfully submitted that the amendments to the specification obviate the objection to the drawings. Specifically, reference number 314 is changed to 312 on page 16 of the specification, and reference number 310 is changed to 309. Further, on page 15, reference number 312 is changed to 310. Accordingly, withdrawal of the objection to the drawings is respectfully requested.

The Office Action objected to the disclosure because of informalities. It is respectfully submitted that the minor errors referred to in the Office Action are corrected. Accordingly, withdrawal of the objection to the disclosure is respectfully requested.

The Office Action objected to claims 5, 7, 9, 11, 14, 19, 25 and 31 because of informalities. It is respectfully submitted that claims 5, 7, 9, 11, 14, 19, 25 and 31 are

amended to correct these informalities. Accordingly, withdrawal of the objection to the claims 5, 7, 9, 11, 14, 19, 25 and 31 is respectfully requested.

The Office Action rejected claims 4-7, 11, 12, 15-20 and 28 under 35 U.S.C. §112, second paragraph, as being indefinite.

As discussed above, claims 4, 15 and 28 are amended to particularly point out and distinctly claim the subject matter of the invention. Specifically, claims 4 and 15 are amended such that the first "it" is replaced by "each upload proxy server" and the second "it" is replaced by "the common destination server." Claim 28 is amended to provide proper antecedent basis for the limitations "unique identifiers," "authenticator" and "corresponding time-stamp."

It is respectfully submitted that all of the claims of the present application particularly point out and distinctly claim the subject matter of the invention. Accordingly, withdrawal of the rejection of claims 4-7, 11, 12, 15-20 and 28 under 35 U.S.C. §112, second paragraph, is respectfully requested.

Claims 1-32 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Number 6, 659,861 to Faris et al. (Faris). This rejection is respectfully traversed.

Claim 1, upon which claims 2-12 depend, recites a method of preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server in the network. The method includes generating a unique identifier corresponding to and dependent on data that each client intends to send to the common destination server, the unique identifier being smaller in size than the data of the

client. The method further comprises separately transmitting the unique identifiers from each client to at least one authenticator trusted by the common destination server and separately time-stamping the unique identifiers as received by the authenticator. The method further comprises separately sending back to each client a message, digitally signed by the authenticator, with the unique identifier sent by that client and the corresponding time-stamp, each client then sending its data towards the common destination server. Further, the method comprises the common destination server using the unique identifier for the data provided by each client to confirm that the data provided by each client existed as of the corresponding time-stamp and to insure that the data has been unaltered after the corresponding time-stamp.

Claim 13, upon which claims 14-22 depend, recites a method of preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server n the network. The method comprises generating a unique identifier corresponding to and dependent on data that each client intends to send to the common destination server, the unique identifier being smaller in size than the data of the client and separately transmitting the unique identifiers from each client to at least one authenticator trusted by the common destination server. The method further includes separately sending back to each client a message, digitally signed by the authenticator, with the unique identifier sent by that client and each client then forwarding its data to the common destination server via proxy upload servers remote from the common destination server. The method further includes the common destination server using the

unique identifier for the data provided by each client to confirm that the data provided by each client has been unaltered after the generation of the unique identifier.

Claim 23, upon which claims 24-28 depend, recites a method of preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server in the network. The method includes providing a common destination server in a network, the common destination server set up to receive data from a plurality of clients. The method further includes providing a plurality of upload proxy servers remote from the common destination server. The method further includes each client sending data, which is intended for the common destination server, to at least a corresponding one of the upload proxy servers. Further, the method includes sending a message, which is smaller in size than the data of a client, to the common destination server to indicate that the common destination server needs to check the corresponding one of the upload proxy servers. Further, the method includes having the common destination server upload the data of a client at some time after the message such that a plurality of clients trying to send data to the common destination server at essentially the same time, is less likely to overload the common destination server and its connection to the network.

Claim 29, upon which claims 30-32 depend, recites a system for preventing upload overloads of data from a plurality of clients at different locations within a network to a common destination server in the network. The system includes a common destination server in a network, the common destination server set up to

receive data from a plurality of clients. The system further includes an id generator operable to generate a unique identifier corresponding to and dependent on data that each client intends to send to the common destination server, the unique identifier being smaller in size than the data of the client. The system further includes each client having a sender for separately transmitting the unique identifier from that client. Further, the system includes at least one authenticator trusted by the common destination server, the authenticator having a time-stamper for separately time-stamping the unique identifiers as received by the authenticator, the authenticator having a sender for separately sending back to each client a message, digitally signed by the authenticator, with the unique identifier sent by that client and the corresponding time-stamp. In the system, the common destination server includes a checker that uses the unique identifier for the data provided by each client to confirm that the data provided by each client existed as of the corresponding time-stamp and to insure that the data has been unaltered after the corresponding time-stamp.

The Office Action alleged that Faris disclosed all of the features of the pending claims. Faris discloses an internet-based system for enabling a time-constrained competition among a plurality of participants over the internet. Faris discloses a plurality of Global Synchronization Unit-enabled client machines, each with a Global Synchronization Unit (GSU). Further, at column 24 lines 34-38, Faris discloses that a client machine is connected to a global synchronization unit (GSU) and at column 36 lines 54-58 discloses that the GSU (alleged authenticator) "generates digitally signed

time and space stamp for the response."

This is in contrast to the features recited in claims 1 and 13. The authenticator is a component of the destination server (see Fig. 5 and page 13 line 25 – page 14 line 4. Thus, the authenticator portion of the destination server sends data with digital signatures to the client. Therefore, the unique identifier and digital signature are performed at the destination server. As discussed above, Faris teaches that the GSU is a part of the client device. Thus, Faris merely discloses that the data produced by the client requires digital signatures in contrast to the preset invention.

It is respectfully submitted that since claims 2-12 and 14-22 depend from claims 1 and 13 respectively, these claims are allowable at least for the same reasons as claims 1 and 13.

Regarding claim 23 as discussed above, claim 23 recites the feature "... each client sending data, which is intended for the common destination server, to at least a corresponding one of the upload proxy servers. . ."

In contrast, there is no indication in Faris that discloses or suggests that each client sends data, intended for primary server 100 (alleged destination server), to at least one game server 150 (alleged proxy server), as recited in claim 23. Instead, Faris merely discloses that the client 160 sends Message 500 to the game server 150, and the security verification log is closed and write protected (see column 37 lines 8-10). In fact, Faris discloses that a separate message 505 ("preliminary results") is sent from the game server 150 to the primary server 100 (see column 38 lines 49-52). Message 505 is

not the original message that has been digitally signed. Thus, there is no disclosure or suggestion in Faris that prevents upload overloads as performed by the present invention.

It is respectfully submitted that since claims 24-28 depend from claim 23, these claims are allowable at least for the same reasons as claim 23.

Regarding claim 29, it is respectfully submitted that Faris fails to disclose or suggest all of the features recited in claim 29. As discussed above, in the present invention the authenticator portion of the common destination server time-stamps the message and separately sends back to each client, a digitally signed message. The client forwards this message to the common destination server.

In contrast, Faris discloses that the GSU is connected to or embedded with the client device. The GSU associated with the client device, which performs the time stamp and digital signature, sends the time-stamped, digitally signed message to the primary server. Thus, it is respectfully submitted that Faris fails to disclose or suggest all of the features recited in claim 29.

It is respectfully submitted that since claims 30-32 depend from claim 29, the claims are allowable at least for the same reasons as claim 29.

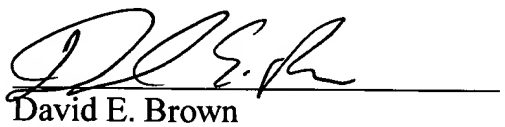
At least in view of the above, it is respectfully submitted that the cited reference fails to disclose or suggest all of the features recited in claims 1-32. Accordingly, withdrawal of the rejection of claims 1-32 under 35 U.S.C. §102(e) is respectfully requested.

Therefore, Applicants respectfully further submit that claims 1-32 of the present application contain allowable subject matter, respectfully request that all claims pending in the present application be allowed, and further request that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:mm